

In re Patent Application of
YANCY ET AL.
Serial No. 10/806,948
Filed: MARCH 23, 2004

In the Claims:

This listing of claims replaces all prior versions and listing of claims in the application.

1. (Currently Amended) A cryptographic device comprising:

a cryptographic module and a communications module coupled thereto;

said cryptographic module comprising a user network interface, a host network processor coupled to said user network interface, and a cryptographic processor coupled to said host network processor;

said communications module comprising a network communications interface coupled to said cryptographic processor;

said host network processor generating cryptographic processor command packets for said cryptographic processor, each comprising an address portion for addressing the cryptographic processor ~~circuit~~ and a data ~~portion~~, portion; and

each data portion including one of unencrypted data and command packets for said communications module;

said host network processor also encapsulating the command packets for said communications module in the data portions of said cryptographic processor command packets;

said cryptographic processor determining if a given cryptographic processor command packet includes the encapsulated

In re Patent Application of
YANCY ET AL.
Serial No. **10/806,948**
Filed: **MARCH 23, 2004**

command packet and based thereon stripping the address portion from each the cryptographic processor command packet and passing the encapsulated communications module command ~~packets~~ packet to said communications module without performing cryptographic processing thereon;

said cryptographic processor determining if another given cryptographic processor command packet includes the unencrypted data packet and encrypting the unencrypted data packet and passing the encrypted data packet to said communications module.

2. (Original) The cryptographic device of Claim 1 wherein said host network processor formats the data portions based upon the simple network management protocol (SNMP).

3. (Original) The cryptographic device of Claim 1 wherein the communications module command packets comprise Ethernet packets.

4. (Original) The cryptographic device of Claim 1 wherein the cryptographic processor command packets comprise Internet protocol (IP) packets.

5. (Original) The cryptographic device of Claim 1 wherein said cryptographic module further comprises:

In re Patent Application of
YANCY ET AL.
Serial No. **10/806,948**
Filed: **MARCH 23, 2004**

a first housing carrying said user network interface,
said host network processor, and said cryptographic processor;
and

a first connector carried by said first housing and
coupled to said cryptographic processor.

6. (Original) The cryptographic device of Claim 5
wherein said communications module further comprises:

a second housing carrying said network communications
interface; and

a second connector carried by said second housing and
being removably mateable with said first connector of said
cryptographic module.

7. (Original) The cryptographic device of Claim 1
wherein said cryptographic processor comprises:

an unencrypted data buffer circuit coupled to said
host network processor;

a cryptography circuit coupled to said unencrypted
data buffer circuit; and

an encrypted data buffer circuit coupled to said
cryptography circuit.

8. (Original) The cryptographic device of Claim 1
wherein said communications module comprises a predetermined one

In re Patent Application of
YANCY ET AL.
Serial No. **10/806,948**
Filed: **MARCH 23, 2004**

from among a plurality of interchangeable communications modules each for communicating over a different communications media.

9. (Original) The cryptographic device of Claim 1 wherein said network communications interface comprises at least one of a wireless LAN (WLAN) communication circuit, a wireline communication circuit, and a fiber optic communication circuit.

10. (Original) The cryptographic device of Claim 1 wherein said user network interface comprises an Ethernet Local Area Network (LAN) interface, and wherein said network communications interface comprises a network LAN interface.

11. (Previously presented) The cryptographic device of Claim 5 wherein said cryptographic module further comprises a tamper circuit for disabling said cryptographic processor based upon tampering with said first housing.

12. (Currently Amended) A cryptographic device comprising:

a cryptographic module and a communications module coupled thereto;

said cryptographic module comprising a user Local Area Network (LAN) interface, a host network processor coupled to said user LAN interface, and a cryptographic processor coupled to said host network processor;

In re Patent Application of
YANCY ET AL.
Serial No. **10/806,948**
Filed: **MARCH 23, 2004**

said communications module comprising a network LAN interface coupled to said cryptographic processor;

said host network processor generating cryptographic processor command packets for said cryptographic processor, each comprising an address portion for addressing the cryptographic processor ~~circuit~~ and a data ~~portion~~, portion; and

each data portion including one of unencrypted data and Ethernet command packets for said communications module;

said host network processor also encapsulating the Ethernet command packets for said communications module in the data portions of said cryptographic processor command packets, said host network processor formatting the data portions based upon the simple network management protocol (SNMP);

said cryptographic processor determining if a given cryptographic processor command packet includes the encapsulated Ethernet command packet and based thereon stripping the address portion from each the cryptographic processor command packet and passing the encapsulated communications module Ethernet command packets packet to said communications module without performing cryptographic processing thereon;

said cryptographic processor determining if another given cryptographic processor command packet includes the unencrypted data packet and encrypting the unencrypted data packet and passing the encrypted data packet to said communications module.

In re Patent Application of
YANCY ET AL.
Serial No. **10/806,948**
Filed: **MARCH 23, 2004**

13. (Original) The cryptographic device of Claim 12 wherein the cryptographic processor command packets comprise Internet protocol (IP) packets.

14. (Original) The cryptographic device of Claim 12 wherein said cryptographic module further comprises:

a first housing carrying said user LAN interface, said host network processor, and said cryptographic processor; and

a first connector carried by said first housing and coupled to said cryptographic processor.

15. (Original) The cryptographic device of Claim 14 wherein said communications module further comprises:

a second housing carrying said network LAN interface;
and

a second connector carried by said second housing and being removably mateable with said first connector of said cryptographic module.

16. (Original) The cryptographic device of Claim 12 wherein said cryptographic processor comprises:

an unencrypted data buffer circuit coupled to said host network processor;

a cryptography circuit coupled to said unencrypted data buffer circuit; and

In re Patent Application of
YANCY ET AL.
Serial No. **10/806,948**
Filed: **MARCH 23, 2004**

an encrypted data buffer circuit coupled to said cryptography circuit.

17. (Original) The cryptographic device of Claim 12 wherein said communications module comprises a predetermined one from among a plurality of interchangeable communications modules each for communicating over a different communications media.

18. (Original) The cryptographic device of Claim 12 wherein said network LAN interface comprises at least one of a wireless LAN (WLAN) communication circuit, a wireline LAN communication circuit, and a fiber optic LAN communication circuit.

19. (Original) The cryptographic device of Claim 12 wherein said user LAN interface comprises an Ethernet interface.

20. (Original) The cryptographic device of Claim 12 wherein said cryptographic module further comprises a tamper circuit for disabling said cryptographic processor based upon tampering with said first housing.

21. (Currently Amended) A communications method comprising:

coupling a cryptographic module to a network device, the cryptographic module comprising a user network interface, a

In re Patent Application of
YANCY ET AL.
Serial No. 10/806,948
Filed: MARCH 23, 2004

host network processor coupled to the user network interface,
and a cryptographic processor coupled to the host network
processor;

providing a communications module comprising a network
communications interface coupled to the cryptographic processor;

causing the host network processor to generate
cryptographic processor command packets for the cryptographic
processor each comprising an address portion for addressing the
cryptographic processor ~~circuit~~ and a data ~~portion~~, portion; and

each data portion including one of unencrypted data
and command packets for the communication module;

the host network processor also to ~~encapsulate~~
encapsulating the command packets for the communications module
in the data portions of the cryptographic processor command
packets; and

causing the cryptographic processor to determine if a
given cryptographic processor command packet includes the
encapsulated command packet and based thereon strip the address
portion from each ~~cryptographic~~ cryptographic processor command
packet and pass the encapsulated communications module command
~~packets~~ packet to the communications module without performing
cryptographic processing thereon; and

causing the cryptographic processor to determine if
another given cryptographic processor command packet includes
the unencrypted data packet and encrypts the unencrypted data

In re Patent Application of
YANCY ET AL.
Serial No. **10/806,948**
Filed: **MARCH 23, 2004**

packet and passes the encrypted data packet to the
communications module.

22. (Original) The method of Claim 21 further comprising causing the host network processor to format the data portions based upon the simple network management protocol (SNMP).

23. (Original) The method of Claim 21 wherein the communications module command packets comprise Ethernet packets.

24. (Original) The method of Claim 21 wherein the cryptographic processor command packets comprise Internet protocol (IP) packets.

25. (Original) The method of Claim 21 wherein the user network interface comprises an Ethernet Local Area Network (LAN) interface, and wherein the network communications interface comprises a network LAN interface.

26. (Currently Amended) A communications system comprising:

a plurality of network devices coupled together to define a network, and a cryptographic device coupled to at least one of said network devices;

In re Patent Application of
YANCY ET AL.
Serial No. **10/806,948**
Filed: **MARCH 23, 2004**

said cryptographic device comprising a cryptographic module coupled to said at least one network device, and a communications module coupled to said cryptographic module;

said cryptographic module comprising a user network interface, a host network processor coupled to said user network interface, and a cryptographic processor coupled to said host network processor;

said communications module comprising a network communications interface coupled to said cryptographic processor;

said host network processor generating cryptographic processor command packets for said cryptographic processor each comprising an address portion for addressing the cryptographic processor ~~circuit~~ and a data ~~portion~~, portion; and

each data portion including one of unencrypted data and command packets for said communications module;

said host network processor also encapsulating the command packets for said communications module in the data portions of said cryptographic processor command packets;

said cryptographic processor determining if a given cryptographic processor command packet includes the encapsulated command packet and based thereon stripping the address portion from each the cryptographic processor command packet and passing the encapsulated communications module command ~~packets~~ packet to said communications module without performing cryptographic processing thereon,

In re Patent Application of
YANCY ET AL.
Serial No. 10/806,948
Filed: MARCH 23, 2004

said cryptographic processor determining if another given cryptographic processor command packet includes the unencrypted data packet and encrypting the unencrypted data packet and passing the encrypted data packet to said communications module.

27. (Original) The system of Claim 26 wherein said host network processor formats the data portions based upon the simple network management protocol (SNMP).

28. (Original) The system of Claim 26 wherein the communications module command packets comprise Ethernet packets, and wherein the cryptographic processor command packets comprise Internet protocol (IP) packets.

29. (Original) The system of Claim 26 wherein said cryptographic module further comprises:

a first housing carrying said user network interface, said host network processor, and said cryptographic processor; and

a first connector carried by said first housing and coupled to said cryptographic processor.

30. (Original) The system of Claim 29 wherein said communications module further comprises:

In re Patent Application of
YANCY ET AL.
Serial No. **10/806,948**
Filed: **MARCH 23, 2004**

a second housing carrying said network communications interface; and

a second connector carried by said second housing and being removably mateable with said first connector of said cryptographic module.

31. (Original) The system of Claim 26 wherein said cryptographic processor comprises:

an unencrypted data buffer circuit coupled to said host network processor;

a cryptography circuit coupled to said unencrypted data buffer circuit; and

an encrypted data buffer circuit coupled to said cryptography circuit.

32. (Original) The system of Claim 26 wherein said communications module comprises a predetermined one from among a plurality of interchangeable communications modules each for communicating over a different communications media.

33. (Original) The system of Claim 26 wherein said network communications interface comprises at least one of a wireless LAN (WLAN) communication circuit, a wireline communication circuit, and a fiber optic communication circuit.

In re Patent Application of
YANCY ET AL.
Serial No. 10/806,948
Filed: MARCH 23, 2004

34. (Original) The system of Claim 26 wherein said user network interface comprises an Ethernet Local Area Network (LAN) interface, and wherein said network communications interface comprises a network LAN interface.

35. (Original) The system of Claim 26 wherein said cryptographic module further comprises a tamper circuit for disabling said cryptographic processor based upon tampering with said first housing.

36. (Currently Amended) A cryptographic module comprising:
a user network interface;
a host network processor coupled to said user network interface; and
a cryptographic processor coupled to said host network processor;

said host network processor generating cryptographic processor command packets for said cryptographic processor each comprising an address portion for addressing the cryptographic processor ~~circuit~~ and a data ~~portion~~, portion; and

each data portion including one of unencrypted data and command packets for said communications module;

said host network processor also encapsulating the command packets for a network communications module in the data portions of said cryptographic processor command packets;

said cryptographic processor determining if a given cryptographic processor command packet includes the encapsulated command packet and based thereon stripping the address portion from each the cryptographic processor command packet and passing the encapsulated communications module command ~~packets~~ packet to the network communications module without performing cryptographic processing thereon;

said cryptographic processor determining if another given cryptographic processor command packet includes the unencrypted data packet and encrypting the unencrypted data packet and passing the encrypted data packet to said communications module.

37. (Previously Presented) The cryptographic module of Claim 36 wherein said host network processor formats the data portions based upon the simple network management protocol (SNMP).

38. (Previously Presented) The cryptographic module of Claim 36 wherein the communications module command packets comprise Ethernet packets.

39. (Previously Presented) The cryptographic module of Claim 36 wherein the cryptographic processor command packets comprise Internet protocol (IP) packets.

In re Patent Application of
YANCY ET AL.
Serial No. **10/806,948**
Filed: **MARCH 23, 2004**

40. (Previously presented) The cryptographic module of Claim 36 wherein said cryptographic processor comprises:

an unencrypted data buffer circuit coupled to said host network processor;

a cryptography circuit coupled to said unencrypted data buffer circuit; and

an encrypted data buffer circuit coupled to said cryptography circuit.

41. (Previously Presented) The cryptographic module of Claim 36 wherein said user network interface comprises an Ethernet Local Area Network (LAN) interface.